

A Management Friendly Transportation SECURITY RISK MANAGEMENT (SRM) Process

By

Lennart E. Long, Security Systems Programs Manager, The Volpe Center

Executive Summary

A Management Friendly Transportation Security Risk Management Process

The National Defense Industrial Association has been working on a quantitative Security Risk Management Process since 1990. David McFadden, the Facilities Security Working Group's Chair has adopted and further developed this Process within the Federal Aviation Administration's FAA Security Division to assess the risk of government assets in terms of dollars for use by the FAA. The FAA team has utilized and further refined this process and is training the FAA Lines of Business in its use and its results. This is being done in order to determine the acceptability of risk of FAA facilities and to rationally and economically meet the requirement of the Presidential Memorandum calling for upgraded security at federal facilities and the Department of Justice Report calling for minimum levels of security at federal facilities.

For more information about this Security Risk Management Process, please call Mr. David C. McFadden at (202) 366-0985 or Mr. Lennart E. Long at (617) 494-2251.

Introduction SRM Requirement

- Presidential Memorandum requires federal facilities to upgrade security
- The requirement for SRM by all Federal agencies is an integral part of the National Performance Review (NPR).
- The Department of Justice report establishes base -line security requirements for reducing vulnerabilities.

Pure Risk Defined

- Pure risk, unlike business and speculative risk, assumes that a threat will be successful.
- This quantifiable damage is referred to as a "loss event".
- The pure risks in every program, project, operation, system, and facility, must be identified as part of the program conceptual design and planning.

Pure Risk

- Some pure risks must be addressed immediately because of their severity and potential for catastrophic impact on the program.
- Other pure risks of a lesser order may be Controlled.
- Others may be accepted by management.

SRM Objective

- The objective of the SRM program is to ensure that the risks from all types of threats, including risks from criminal and terrorist attacks, are reduced to an acceptable level through the application of cost effective countermeasures.

What is SRM?

- SRM is the logical process that is used to determine:
 - What risks are acceptable
 - What risks are unacceptable
 - What type and extent of countermeasures are required
- SRM is a dynamic and interactive process.
- SRM must be part of the life cycle of every program, project, operation, system, and facility.

SRM Purpose

- To evaluate the risk to the facility in terms of its critical assets
- To quantify risk and establish what risks are unacceptable
- To determine what measures and costs are required to reduce unacceptable risks to an acceptable level

SRM Scope

- SRM must be part of all Program Implementation plans, funding profiles, and Mission Needs Statements
- The SRM program must be part of the acquisition life cycle from the Mission Needs to the procurement and throughout the effective operational life of the asset.

SRM Goals

- Provide cost effective risk reduction
- Accept some risk, and ensure that prudent security measures are used in all facilities

Concept of Asset

- Assets are anything of value to the NAS mission including equipment, personnel, equipment, and procedures
- Each asset has pure risk
- To evaluate pure risk, assets must be quantified in terms of dollars

SRM Asset Identification

- Identification of Assets
 - Specific Assets need to be addressed
 - Each asset is evaluated in terms of its:
 - Value in dollars

- Replacement cost
- The impact of dollars that would result from the loss or damage of an asset

SRM Determine Criticality

- Once the asset is identified and quantified, a determination must be made regarding its criticality.
- Criticality is quantified in terms of impact of loss in dollars if the asset is damaged or destroyed.
- Assigning a criticality rating permits prioritization of assets
- Assign a criticality rating by arranging assets in order of priority with the most critical first and the least critical last.

•Criticality Designator 1 – Catastrophic

- Total Destruction or Loss of the asset or sufficiently severe damage to the asset causing complete loss of mission capability for an extended period

Criticality Designator 2 – Very Serious

- Major damage to the asset requiring extensive repairs with consequent severe impairment of the mission capability

•Criticality Designator 3 – Moderately Serious

- Damage of the asset is sufficient to require immediate repairs with noticeable impact of the capability of the facility to accomplish its mission

•Criticality Designator 4 – Not Serious

- Damage to the asset is such that there is no noticeable adverse impact on the capability of the facility to perform its mission

•-----

•SRM Threat Considerations

- - Determine what threats are associated with each asset
 - Evaluate all known threats
 - The threat evaluation shall include information from prior risk assessments if available
 - Information from intelligence agencies

•SRM Existing Countermeasures

- Current and planned countermeasures are identified and quantified as to their effectiveness in reducing risk

•-----

•SRM Determine Vulnerability

- Identify and quantify vulnerabilities for all assets

•-----

•

•Vulnerability Rating A – Certain

- Given no changes, the loss event will occur.

•-----

Vulnerability Rating B – High Probability

- The loss event is much more likely to occur.

•-----

.Vulnerability Rating C – Moderately Probable

- The loss event is more likely to occur

•-----

.Vulnerability Rating D – Improbable

- The loss event is not likely to occur

•-----

.SRM Risk Logic

- Determine the Risk Level by combining
 - Criticality Designator (1-4) and
 - Vulnerability Rating (A-D)

•-----

•SRM Risk Logic – Impact of Loss

- See Process Chart below

•-----

•SRM Risk Logic

- Determine acceptability of risk by interpretation of Impact of Loss data

•-----

•Risk Logic – Risk Management Guide

- See Process Chart below

•-----

•Develop Countermeasures

- Evaluate all risk reduction measures for reducing unacceptable risks to acceptable levels

•-----

•Perform Cost/Benefit Analysis

- Cost benefit analysis results are arranged in priority order according to their effectiveness
 - Assemble data
 - Review forcing functions
 - Review benefits
 - Review costs for alternate countermeasures

- Estimate percentage of risk reduction for each countermeasure
- Calculate value of benefit
- Calculate cost/benefit ratio
- Compare
- Select or reject
- Repeat until acceptable upgrades are identified

•-----

•Proceed with upgrade

- The most cost-effective countermeasures are recommended to management in the SRM Assessment Report

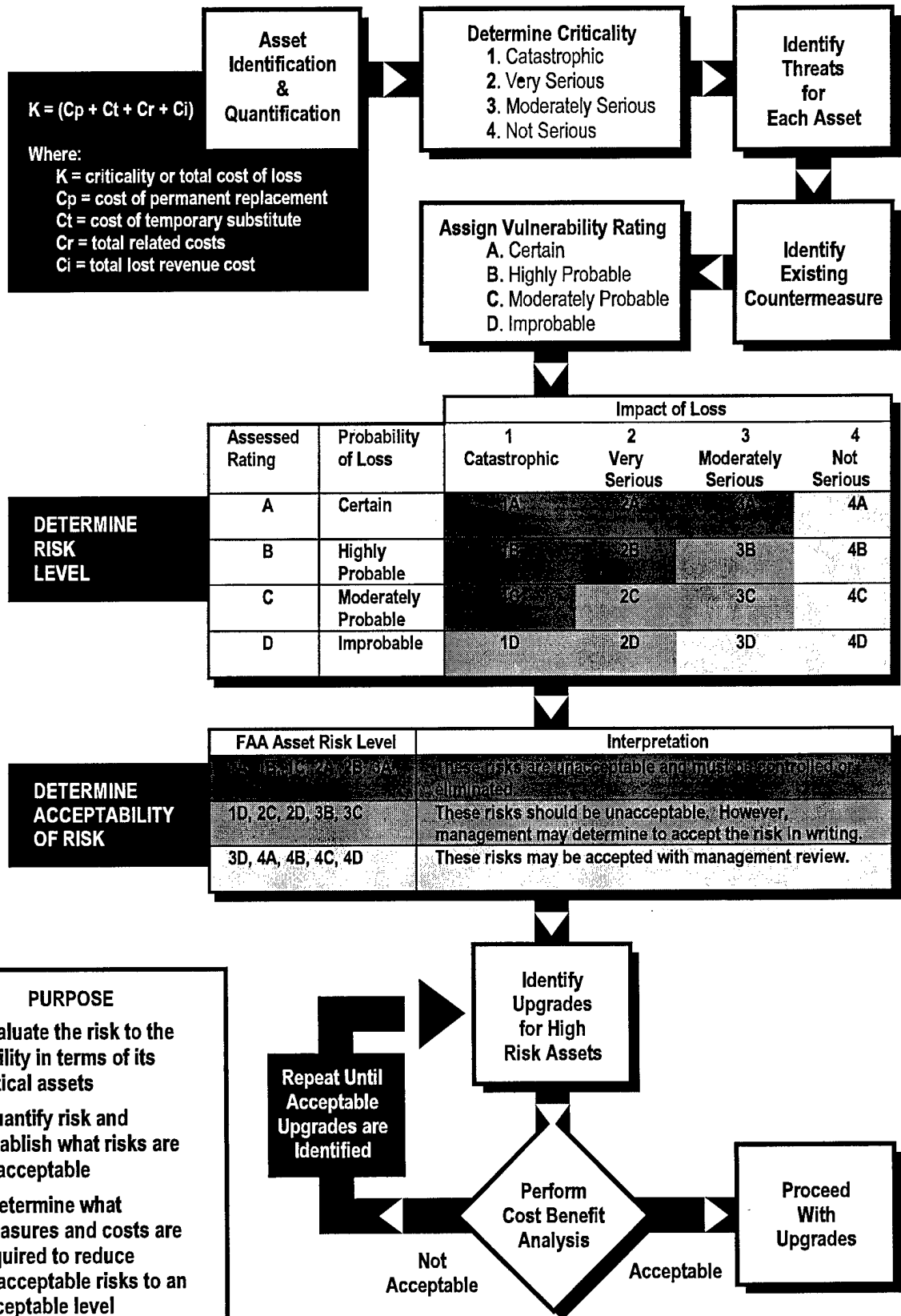
•

•

Summary

- Through the SRM process, resources and funds are concentrated on the most critical assets, and on the risks that pose the greatest danger to mission and people.

FAA SECURITY RISK MANAGEMENT PROCESS



End of Presentation

This presentation is the product of the Volpe Center. The sponsor of this product is the Federal Aviation Administration.

For more information, contact:

Lennart E. Long

617-494-2251